IN THE CLAIMS:

Claim 1 (Currently Amended) A method of ~~encrypting and decrypting~~ for securely storing an electronic data file ~~on a web-based computer system~~, comprising:

~~receiving, by~~ transmitting to a computer system, an electronic data file, wherein the computer system ~~includes~~ comprises a memory subsystem and a plurality of memory locations;

encrypting the data file in the memory subsystem; and

storing the encrypted data file in the one or more ~~of the plurality of~~ memory locations,

wherein encrypting the data file occurs without assistance from a user and without requiring the user's knowledge of the algorithm used to encrypt the data file~~;~~

~~retrieving the encrypted data file from the one or more memory locations;~~

~~decrypting the encrypted data file in the memory subsystem; and~~

~~displaying the decrypted data file on a web browser~~.

Claim 2 (Currently Amended) The method of claim 1 further comprising~~, prior to the receiving step~~:

~~receiving a username and a password from an external user device; and~~

verifying the ~~username and password correspond to a pre-defined user having~~ user is authorized to access ~~to~~ the computer system.

Claim 3 (Currently Amended) The method of claim 1 further comprising~~,~~ ~~between the storing step and the retrieving step~~:

retrieving the encrypted data file from the one or more memory locations;

~~analyzing the encrypted data file;~~

decrypting the data file;

modifying the decrypted ~~analyzed~~ data file;

re-encrypting the data file; and

storing the modified data file in the one or more memory locations, wherein the decrypting and re-encrypting occur without assistance from the user and without requiring the user's knowledge of the algorithm used to encrypt the data file.

Claim 4 (Currently Amended) The method of claim 1 wherein the ~~receiving~~ transmitting step is performed using a SSL/HTTPS protocol.

Claim 5 (Cancelled)

Claim 6 (Original) The method of claim 1 wherein the memory subsystem includes random access memory.

Claim 7 (Currently Amended) A method ~~of encrypting and decrypting~~ for securely storing an electronic data file ~~on a web-based computer system~~, comprising:

~~receiving, by a web server~~ transmitting to a first computer system, an electronic data file, wherein the ~~web server includes~~ first computer system comprises a memory subsystem;

encrypting the data file in the memory subsystem;

transmitting the encrypted data file to a ~~file server~~ second computer system having a plurality of memory locations; and

storing the encrypted data file in one or more of the ~~plurality of~~ memory locations,

wherein encrypting the data file occurs without assistance from a user and without requiring the user's knowledge of the algorithm used to encrypt the data file~~;~~

~~retrieving the encrypted data file from the one or more memory locations;~~

~~transmitting the encrypted data file to the web server;~~

~~decrypting the encrypted data file in the memory subsystem; and~~

~~displaying the decrypted data file on a web browser~~.

Claim 8 (Currently Amended) The method of claim 7 further comprising~~, prior to the receiving step~~:

~~receiving, by the web server, a username and a password from an external user device; and~~

verifying~~, by the web server, the username and password correspond to a pre-defined user having~~ the user is authorized to access ~~to~~ the first computer system.

Claim 9 (Currently Amended) The method of claim 7 further comprising~~, between the storing step and the retrieving step~~:

retrieving the encrypted data file from the one or more memory locations;

~~analyzing the encrypted data file;~~

decrypting the data file;

modifying the decrypted ~~analyzed~~ data file;

re-encrypting the data file; and

storing the modified data file in the one or more memory locations, wherein the decrypting and re-encrypting occur without assistance from the user and without requiring the user's knowledge of the algorithm used to encrypt the data file.

Claim 10 (Original) The method of claim 7 wherein the receiving step is performed using a SSL/HTTPS protocol.

Claim 11 (Cancelled)

Claim 12 (Original) The method of claim 7 wherein the memory subsystem includes random access memory.

Claim 13 (Currently Amended) The method of claim 7 further comprising~~,~~ ~~between the storing step and the retrieving step~~:

retrieving the encrypted data file from the one or more memory locations;

transmitting the encrypted data file to a ~~back-end data processing server~~ third computer system;

~~analyzing, by the back-end data processing server, the encrypted data file;~~

decrypting the data file on the third computer system;

modifying, ~~by the back-end data processing server~~, the encrypted ~~analyzed~~ data file;

re-encrypting the data file on the third computer system;

transmitting the modified data file to the ~~file server~~ second computer system; and

storing the modified data file in the one or more memory locations.

Claims 14 (Currently Amended) A system for ~~encrypting and decrypting~~ transferring an electronic data file, comprising:

a ~~web server~~ first computer system for encrypting a data file and decrypting an encrypted data file, the ~~web server~~ first computer system having a memory subsystem; and

a ~~file server, electrically connected to the web server, for storing the encrypted data file, the file server~~ second computer system in communication with the first computer system, the second computer system having a plurality of memory locations~~; and~~

~~a back-end data processing server, electrically connected to the file server, for modifying~~ configured to store the encrypted data files,

wherein the ~~web server includes a computer process comprising~~ first computer system is configured to:

~~receiving~~ receive the data file from ~~an external~~ a user device,

~~encrypting~~ encrypt the data file in the memory subsystem without interaction from a user and without requiring the user's knowledge of the algorithm used to encrypt the data file, and

transmit~~ting~~ the encrypted data file to the ~~file server~~ second computer system,

wherein the ~~file server includes a computer process comprising~~ second computer system is configured to:

~~receiving~~ receive the encrypted data file from the ~~web server~~ first computer system, and

~~storing~~ store the encrypted data file in one or more ~~of a plurality of~~ memory locations~~,~~

~~retrieving the encrypted data file from the one or more memory locations, and~~

~~transmitting the encrypted data file to the back-end processing server,~~

~~wherein the back-end data processing server includes a computer process comprising:~~

~~receiving the encrypted data file from the file server,~~

~~analyzing the encrypted data file,~~

~~modifying the analyzed data file, and~~

~~transmitting the modified data file to the file server.~~

Claim 15 (Currently Amended) The system of claim 14 wherein the ~~computer process of the file server further comprises~~ second computer system is further configured to:

~~receiving the modified data file from the back-end data processing server;~~

~~storing the modified data file in the one or more memory locations;~~

~~retrieving~~ retrieve the ~~modified~~ encrypted data file from the one or more memory locations; and

transmit~~ting~~ the ~~modified~~ encrypted data file to the ~~web server~~ first computer system.

Claim 16 (Currently Amended) The system of claim ~~15~~ 14 wherein the ~~computer process of the web server further comprises~~ first computer system is further configured to:

~~receiving~~ receive the ~~modified~~ encrypted data file from the ~~file server~~ second computer system; and

decrypt~~ing~~ the ~~modified~~ encrypted data file in the memory subsystem~~; and~~

~~displaying the decrypted data file on a web browser~~,

wherein decrypting the encrypted data file occurs without interaction with a user and without requiring the user's knowledge of the algorithm used to decrypt the encrypted data file by the user.

Claim 17-21 (Cancelled)

Claim 22 (New) The method of claim 1 further comprising:

retrieving the encrypted data file from the one or more memory locations;

decrypting the data file; and

providing the user access to the data file, wherein the decrypting occurs without assistance from the user and without requiring the user's knowledge of the algorithm user to encrypt the data file.

Claim 23 (New) The method of claim 7 further comprising:

retrieving the encrypted data file from the one or more memory locations;

decrypting the data file; and

providing the user access to the data file, wherein the decrypting occurs without assistance from the user and without requiring the user's knowledge of the algorithm user to encrypt the data file.

Claim 24 (New) The system of claim 14 wherein the second computer system is further configured to:

retrieve the encrypted data file from the one or more memory locations;

decrypt the data file;

modify the decrypted data file;

re-encrypt the data file; and

store the modified data file in the one or more memory locations.

Claim 25 (New) The system of claim 14 further comprising:

a third computer system in communication with the second computer,

wherein the second computer system is further configured to:

retrieve the encrypted data file from the one or more memory locations,

transmit the encrypted data file to the third computer system,

receive a modified data file from the third computer system, and

store the modified data file in the one or more memory locations, and

wherein the third computer system is configured to:

receive the encrypted data file from the second computer,

decrypt the data file,

modify the decrypted data file,

re-encrypt the data file, and

transmit the modified data file to the second computer.

Claim 26 (New) A system for securely storing an electronic data file comprising:

a receiving subsystem configured to receive a data file from a user device;

an encrypting subsystem configured to encrypt the data file;

a plurality of memory locations configured to store an encrypted data file in one or more memory locations;

a decrypting subsystem configured to decrypt the encrypted data file; and

a display subsystem configured to display the decryption file.

wherein the encrypting subsystem operates to encrypt the data file without assistance from a user and without requiring the user's knowledge of the algorithm used to encrypt the data file, and

wherein the decrypting subsystem operates to decrypt the encrypted data file without assistance from a user and without requiring the user's knowledge of the algorithm used to encrypt data file.

Claim 27 (New) A method for accessing a secure electronic file on a computer system, comprising:

retrieving, from a computer system having a memory subsystem and a plurality of memory locations, an encrypted data file from one or more memory locations;

decrypting the encrypted data file in the memory subsystem; and

providing access to the decrypted data file, wherein decrypting the encrypted data file occurs without assistance from a user and without requiring the user's knowledge of the algorithm used to encrypt the data file.

Claim 28 (New) The method of claim 27 further comprising:

modifying the decrypted data file;

encrypting the modified data file; and

storing the encrypted modified data file in the one or more memory locations, wherein the encryption of the modified data file occurs without assistance from a user and without requiring the user's knowledge of the algorithm used to encrypt the data file.

Claim 29 (New) The method of claim 27 wherein the memory subsystem includes random access memory.

Claim 30 (New) A method for securely accessing an electronic data file comprising:

retrieving, from a first computer system comprising a plurality of memory locations, an encrypted data file from one or more of the memory locations;

transmitting the encrypted data file to a second computer system comprising a memory subsystem;

decrypting the encrypted data file in the memory subsystem; and

displaying the decrypted data file,

wherein decrypting the encrypted data file occurs without assistance from a user and without requiring the user's knowledge of the algorithm used to encrypt the data file.

Claim 31 (New) The method of claim 30 further comprising:

transmitting the encrypted data file to a third computer system;

decrypting the encrypted data file;

modifying, by the third computer system, the data file;

encrypting the modified data file;

transmitting the encrypted modified data file to the first computer system; and

storing the modified data file in the one or more memory locations.

Claim 32 (New) The method of claim 30 further comprising:

retrieving the encrypted data file from the one or more memory locations;

decrypting the encrypted data file;

modifying the data file;

encrypting the modified data file; and

storing the encrypted modified data file in the one or more memory locations.

Claim 33 (New) The method of claim 30 wherein the memory subsystem includes random access memory.

Claim 34 (New) A system for securely storing electronic data files comprising:

means for receiving a data file;

means for encrypting the data file;

means for storing the encrypted data file;

means for retrieving the stored data file;

means for decrypting the retrieved data file; and

means for displaying the decrypted data file.

Claim 35 (New) The method of claim 34 further comprising:

means for modifying the retrieved data file;

means for encrypting the modified data file; and

means for storing the encrypted modified data file.